Global Tides and Currents of Maritime Domain Awareness

The rise of transnational threats.

by CDR JIM ROBBINS
International Coordination, U.S. Coast Guard Maritime Domain Awareness Directorate

Consider these frightening, but fortunately, fictional scenarios: A bulk carrier is blown up in Rotterdam. A ship offloads a container in Montreal that holds toxic chemicals intended to poison a North American water supply. An oil tanker breaks apart and disgorges its contents onto the Great Barrier Reef. A longliner fishing vessel uses banned equipment, killing mammals and sea turtles while it harvests its targeted species. An absconder comes ashore in a U.S. port, while shore authorities are diverted by a false-positive indication for nuclear material on an arriving vessel. A barge containing ammonia nitrate explodes as it passes through a major city. A remotely controlled aircraft departs a vessel at sea to deliver an improvised explosive device. A small boat laden with explosives loiters, awaiting the arrival of a cruise ship.

A fertile mind could invent many more scenarios that could challenge the international maritime community. It was not so long ago that even the most fantastic of fiction writers would have rejected situations such as these. Unfortunately many of these worrisome scenarios are now thought of as not only realistic but, in some cases, likely.

While all the scenarios are different, they all have a couple things in common. First, they all take place in and around the world's waterways. The other commonality is that all of these problematic scenarios involve transnational threats—problems that cross national boundaries. A list of transnational threats would include piracy, illegal migration, narcotics smuggling, terrorism, illegal fishing, weapons smuggling, weapons of mass destruction proliferation, and threats to the environment.

Transnational threats are nothing new, so why have they become so significant now? The reason is partially the result of a diminished threat from nation states, but perhaps the biggest reason that transnational threats now garner the attention of national leaders is the unprecedented empowerment of individuals and small groups. Advances in technology have allowed individuals, no matter how dispersed or remotely located, to access detailed information on any subject and collaborate on nefarious acts without a supporting local population or a sophisticated infrastructure. The Oklahoma City bombing and the terrorist events of September 11, 2001 are obvious examples.

Countering Transnational Threats
Of course, these threats are extremely widespread and vulnerabilities abound. So, how does one effectively counter them? One of the most obvious answers is cooperation with other nations, and an obvious and potentially very fruitful form of cooperation is information sharing. Part of the nature of transnational threats is their direct relationship to national boundaries and seams between jurisdictions. Those who would perpetrate these threats may exploit seams and circumvent conventional areas of surveillance—working "below the radar."

This ability for transnational threats to take advantage of these seams and boundaries forces us to seek ways to subdue or blur these boundaries to a point where the adversary can no longer use them to their advantage. This leads us to cooperation, principally information sharing, and, by extension, global information sharing, which is a foundational concept of Maritime Domain Awareness (MDA).

To counter transnational maritime threats, we must know and understand, on a global scale, activities in the maritime domain. Therefore, MDA is an essential element of any maritime security strategy. The "National Strategy for Maritime Security" also articulates the strategic importance of MDA (see related article in this edition).

Civil/Military Partnership

To make global coordination and sharing of information effective, national governments must put in place an essential partnership between civil and military maritime authorities. This basic partnership is a prerequisite for a viable national approach to MDA, since many of the seams that give rise to transnational threats are between elements of the same government.

Both civil and defense interests are important in a holistic approach to Maritime Domain Awareness. The world's militaries have extensive maritime command and control infrastructures, as well as vast information architectures. Much of the nonvoluntary maritime surveillance data originates from military systems, and additionally, it is often a nation's military that is viewed as the best agent for collecting and disseminating maritime information in a trustworthy, apolitical, and efficient manner. A nation's civil maritime agencies, on the other hand, are intimately involved in day-to-day maritime activities and interact as a matter of course with the full spectrum of maritime players. Civil agencies understand the impact of security measures on commercial operators and have a vested interest in ensuring that security practices are integrated in such a way as to not disrupt the efficient flow of commerce.

As the regulators and enforcers, the civil agencies know a great deal about what goes on in the maritime domain and can give value to the military's information. And from an operational point of view, it will be law enforcement agencies, in the vast majority of scenarios, who are expected to act against a threat. Ultimately, what must be arrived at is a marriage between the primary government entities that execute civil and military maritime functions, and it is the resulting fused information set that brings value to international maritime partnerships.

Why is Achieving MDA so Hard?

Building the necessary partnerships on which MDA relies is difficult and can take some time. The inclusive nature of MDA can be overwhelming—like eating the proverbial elephant. A strategy to achieve MDA requires bite-size initiatives, but this bite-size strategy

can lead to, at least temporarily, the exclusion of important elements. This dilemma can cause programs to languish, due to lack of the perfect solution. A clear vision with broad support from leaders in key positions is necessary to remedy this problem and ensure that progress continues.

Sharing and partnerships involve compromise and are, by their very nature, risky ventures that require a great deal of work. Stakeholders participate in cooperative ventures only if they see tangible benefits, and it is rare for anyone to give something away without expecting something in return. Sometimes the "return" on a partnership is hard to quantify, especially early on. "Because it is right" is rarely a convincing argument to win funding or inspire parochial interests into action.

Within and among organizations there are inevitable conflicts as to roles and responsibilities. Multiple agencies interests can be difficult to assimilate. Governments sometimes are faced with a situation where they must designate one lead agency among several competing agencies. An alternative might be to bestow information-sharing authority to an intragovernmental body, however this becomes problematic when statutory authorities of individual departments and agencies are considered. It would be difficult, for instance, for a multiagency body to negotiate with foreign governments.

In addition, many countries have significant legal obstacles to sharing information among their own government entities. Add to this the predisposition of most organizations to work within their own walls rather than seek partnerships, and it becomes apparent that there is a great deal of bureaucratic intransigence to overcome. Lastly, the processing and distribution of information requires information technology infrastructure, and new requirements for technology capabilities cost money. Redirecting scant resources toward new information technology solutions requires compelling reasons and significant political will.

These considerable challenges can be overcome, but sometimes not within the attention span of political leaders. Achieving an effective understanding of the maritime domain is a continual process that will require many years.

Global Progress

Many examples of international MDA exist now, representing the full spectrum of maritime mission areas and originating from both national and multina-

A USCG senior delegation meets with Chinese delegation to discuss maritime security. The delegation includes, second from right, ADM T. H. Collins (then USCG Commandant) and center, VADM H. E. Johnson. USCG photo.

tional sponsors. The Automated Mutual Assistance Vessel Rescue (Amver) system and other vessel reporting systems track commercial vessels through satellite systems and are used globally by search and rescue authorities and shipping companies to monitor vessel movements. Some cooperative arrangements are already in place among different vessel reporting systems. Vessel reporting systems are envisioned as providing the necessary access to long-range identification and tracking data, as provided for in the recent amendment to the International Safety of Life at Sea Convention. This new amendment allows nations to have access to ship position data if the vessel is either bound for one's port, flies one's flag, or is operating within 1,000 nautical miles of one's coast.

Many regional efforts are in the works. The Malaccan straits forms the main maritime passageway between the Indian Ocean and the Pacific Ocean, linking three of the globe's most populous countries: India, Indonesia, and China. It is the focus of a host of initiatives, including U.S. Pacific Command's Comprehensive Maritime Awareness project with Singapore; the MALSINDO (Malaysia, Singapore, and Indonesia) coordinated security effort; the Marine Electronic Highway project; and the regional cooperation agreement on combating piracy and armed robbery against ships in Asia. It is hoped that systems, processes, and policies implemented in the Malaccan straits region can be exported and replicated in other locations around the world that face similar challenges.

Other global regions have significant efforts, as well. In the Mediterranean, the Italian Navy sponsors a virtual regional maritime traffic center, which takes reports of civil vessel movements via Navy command

centers throughout the Mediterranean region and fuses the information for redistribution to all participating nations. European-focused initiatives are underway in the European Union, NATO, and U.S. European Command. In the North Pacific, the North Pacific Coast Guards Automated System is in place and operating, allowing the exchange of maritime information directly among all member nations.

The Way Ahead
Maritime Domain Awareness is a transformational concept that represents a fundamental change in the way maritime challenges are approached. A change of this magnitude does not occur overnight and requires a continual effort. Building trust between and among nations and national entities takes time and effort. As we refine our strategy, policy, and capability requirements, we will implement incremental improvements.

For the Coast Guard's part, we are establishing servicewide information-sharing requirements in support of the "National Strategy for Maritime Security" and are pursuing information-sharing protocols with a number of strategic partners. For the time being, the Coast Guard is likely to seek unique relationships with each partner nation, but ultimately, bilateral efforts should evolve into regional accords and global standards for information exchange. We will work to support the initiatives that will lead to a globally interconnected maritime information system that is responsive to all threats, promotes transparency and trust between nations, preserves personal freedoms, and facilitates commerce.

About the author: CDR Robbins recently retired from the Coast Guard after more than 20 years of service. CDR Robbins' career consisted primarily of tours as a C-130 and H-60 aircraft commander and instructor pilot. He is a recipient of the Meritorious Service Medal and the Coast Guard Commendation Medal.